

	RECORDS MANAGEMENT SYSTEM (RMS) ACCESS	Operations Order 5.3.01
	PHOENIX POLICE DEPARTMENT	Rev. 10/15 PAGE 1

1. GENERAL INFORMATION

- A. This policy applies to authorized personnel who access RMS information, and Arizona Criminal Justice Information System (ACJIS) and Arizona Crime Information Center (ACIC)/National Crime Information Center (NCIC) information through the Centrally Linked Information for Public Safety (CLIPS™) application.
- B. Only personnel with a Terminal Operator Certification (TOC) are allowed access to RMS or CLIPS™ which contains confidential and personal identifying information.
- C. Fingerprint based criminal history and stringent background checks are required for all personnel who access RMS or CLIPS™.
- D. The Department is considered an “interface agency” to the Arizona Department of Public Safety (DPS) and the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division and is therefore subject to rules and regulations imposed by those agencies.

2. RMS OR CLIPS™ ACCESS

- A. RMS or CLIPS™ access will be:
 - Based upon the user’s role within the Department.
 - Authorized based on the least privilege required to perform assigned tasks.
 - Granted only if approved by the supervisor of the user and System Security Officer (SSO).
 - Authorized only if the user has undergone fingerprint based background checks (state and federal) with no criminal history that would preclude employment
- B. All personnel authorized to access RMS or CLIPS™ must obtain a Level A, B, C, D, or E TOC issued by DPS, based on the user’s role within the Department.

NOTE: Authorized personnel must renew their TOC every two years.

- C. RMS or CLIPS™ access is limited to law enforcement related responsibilities/duties.
- D. Requests – All requests for RMS or CLIPS™ access or updates to RMS or CLIPS™ access must be documented on the RMS or CLIPS™ Access Request Form 80-581D.
 - (1) The RMS or CLIPS™ Access Request form must be:
 - (a) Approved by the user’s immediate supervisor.
 - All requests for “Locked” access must also be approved by the user’s commander/administrator **and** the commander/administrator of the “locked unit/bureau”.
 - (b) Submitted to the SSO in the Information Services Unit (ISU).
 - (c) Retained for the life of the user’s employment.
- E. Transfers – When personnel are reassigned or transferred to other positions within the Department, appropriate actions such as, closing or establishing accounts and changing access authorizations, will occur upon notification of the transfer.
- F. Retirements/Terminations - Upon notification of an authorized user’s retirement/termination, authorized personnel or processes will disable all user IDs.

	RECORDS MANAGEMENT SYSTEM (RMS) ACCESS	Operations Order 5.3.01
	PHOENIX POLICE DEPARTMENT	Rev. 10/15 PAGE 2

2. G. Misuse of RMS or CLIPS™ Access - The Professional Standards Bureau (PSB) will investigate all alleged misuse of the RMS or CLIPS™ and/or the information contained within RMS or CLIPS™.

3. **RMS OR CLIPS™ USER ACCOUNTS**
 - A. A “User” account will be established for each authorized user requiring access to RMS or CLIPS™ and each account will have a unique user identification (ID).
 - (1) Authorized users include:
 - (a) Department employees including reserve officers
 - (b) City employees: City Prosecutor’s Office, City Court, and Fire Department personnel
 - (c) Non-employees:
 - Interns and in some cases, consultants and contractors when start and end dates are known
 - Temporary personnel on contract from a temporary service agency assigned to supplement existing staff
 - Volunteers working set hours and days for an unknown length of time
 - B. RMS or CLIPS™ will authenticate each user’s identity in a manner consistent with RMS’s or CLIPS’s protection requirements.
 - Advanced authentication will be utilized when remotely accessing the Department’s network, RMS, or CLIPS™.
 - C. For systems containing personally identifying or restricted law enforcement information, the system will force an automatic lock-out after three (3) unsuccessful logon attempts.
 - User access will be reactivated by the SSO or authorized personnel in ISU after verifying the user’s identity.

4. **SUSPENDING USER ACCOUNTS** – If necessary, authorized personnel or processes will suspend user accounts after 60 days of non-use.
 - User accounts will be reactivated by an ISU supervisor after verifying the user’s identity.

5. **OTHER SYSTEMS ACCESS** – Authorized RMS or CLIPS™ users may also have access to Arizona Computerized Criminal History (ACCH), Coplink, and Arizona Motor Vehicle Division (MVD) information.

6. **REQUESTS FROM OTHER AGENCIES TO ACCESS RMS** - Other local law enforcement agencies requesting to utilize RMS will be approved if all of the below apply:
 - A. There is an up-to-date Intergovernmental Agreement (IGA) between the Department and the requesting agency
 - B. The requesting agency is a certified law enforcement agency
 - C. The requesting agency’s personnel have TOC numbers issued by DPS.

7. **COMPLIANCE AUDITS** – The City Auditor Department may conduct periodic audits to evaluate compliance with the requirements set forth in this order.

	RECORDS MANAGEMENT SYSTEM (RMS) ACCESS	Operations Order 5.3.01
	PHOENIX POLICE DEPARTMENT	Rev. 10/15 PAGE 3

Last Organizational Review: